NETSEC.CO
THE NETWORK SECURITY COMPANY

Schulung *Kryptografie/Zertifikate*

Factsheet

THEMA	Grundlagen Kryptografie und Zertifikate
KURZBESCHREIBUNG	Viele Sicherheitstechnologien in der IT basieren auf kryptografischen Verfahren. Dieses Modul startet mit einer Einführung der wichtigsten Verfahren und vertieft dann mit konkreten Anwendungen wie Verschlüsselung, digitale Signatur, Zertifikate und sichere Transportprotokolle.
ZIELGRUPPE	IT Spezialisten, Softwareentwickler
VORAUSSETZUNG	Grundkenntnissen in Softwareentwicklung, Mathematik Sekundarstufe II
AUFBAUENDE MODULE	-
DAUER	1 Halbtag, inkl. Fragen und Diskussion
KURSART	Frontalschulung, Praxisbeispiele, Demos, Diskussion

Inhalt

- Symmetrische und asymmetrische Verschlüsselung
- Hash Funktionen
- digitale Signatur
- asymmetrische Verschlüsselung am Beispiel RSA
- sichere Transportprotokolle (SSL/TLS)
- Identifikation, *Trust Chain*
- Zertifikate
- Smartcard, TPM und HSM
- Praktische Anwendung kryptografischer Verfahren

Ziele

Nach der Absolvierung des Moduls wissen die Teilnehmenden, was eine Hash Funktion ist und wie eine digitale Signatur funktioniert. Sie kennen den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren, wissen welche Arten von Zertifikaten es gibt und wozu diese dienen. Weiter wissen sie, worauf bei der Anwendung kryptografischer Verfahren zu achten ist und welche Anforderungen an den Umgang und die Speicherung von Schlüsselmaterial zu stellen sind.